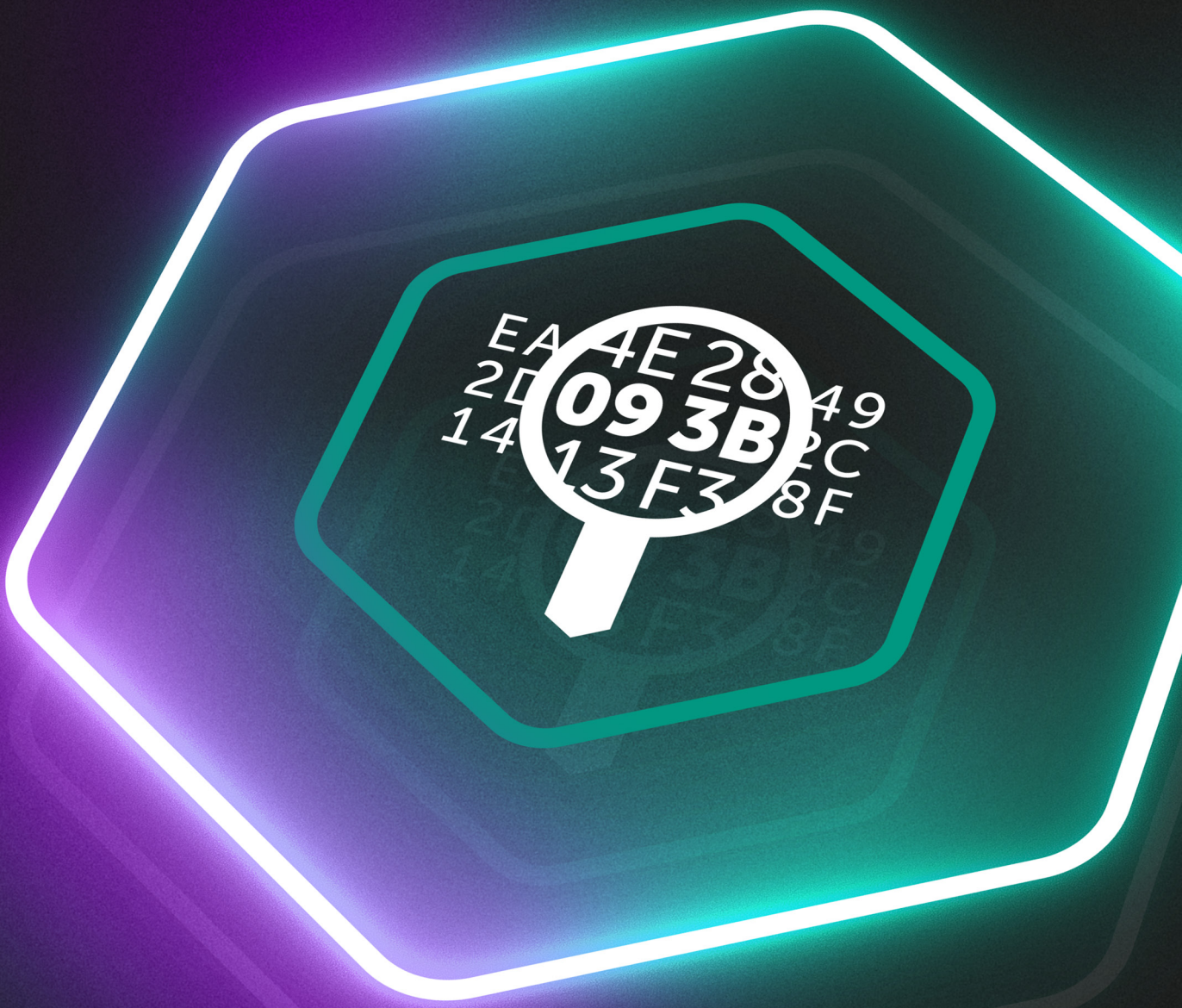


Kaspersky Threat Lookup

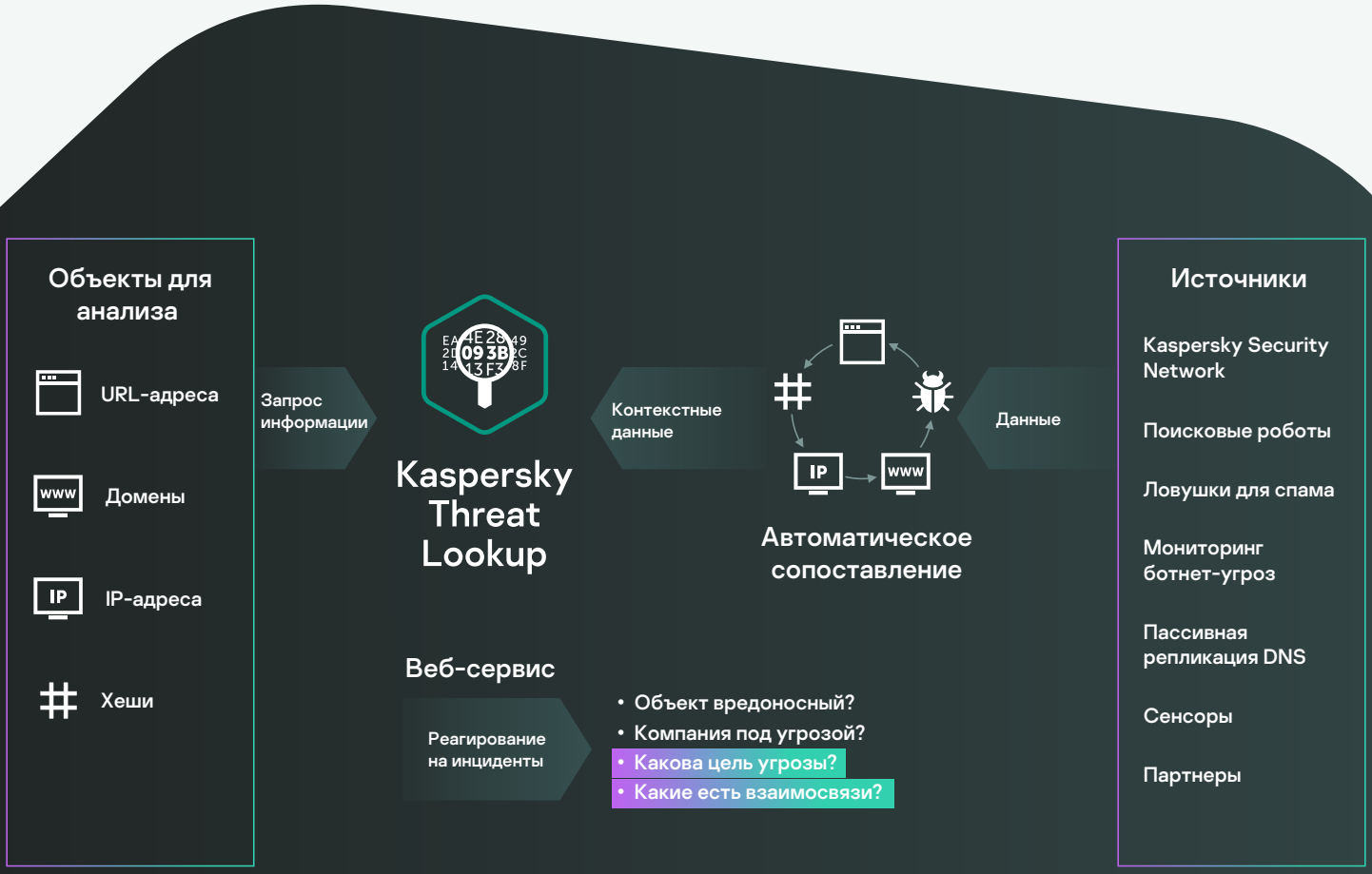
Kaspersky Threat Lookup
Поисковый портал о киберугрозах и их взаимосвязях

Киберпреступность не знает границ, а ее техническая база быстро совершенствуется. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение рабочих процессов, кражу активов и нанесение ущерба, злоумышленники используют сложные цепочки поражения, а также специально подобранные тактики, техники и процедуры.

Kaspersky Threat Lookup – это мощная единая онлайн-платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Портал предоставляет самые последние данные по веб-адресам, доменам, IP-адресам, хешам файлов, названиям угроз, статистическим и поведенческим данным, данным WHOIS / DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и прочему. Результатом является глобальная видимость новых и возникающих угроз, что помогает защитить организацию и ускоряет реагирование на инциденты.

Запрос пробного доступа к Kaspersky Threat Lookup

Подробнее



Преимущества

Надежные данные об угрозах: «Лаборатория Касперского» предоставляет надежные данные об угрозах детальной контекстной информацией. Продукты «Лаборатории Касперского» демонстрируют наилучшие результаты при тестировании решений для защиты от вредоносных программ. Непревзойденное качество аналитических данных подтверждается высоким уровнем обнаружения с минимальным уровнем ложных срабатываний.

Поиск угроз: проактивный подход к предотвращению и обнаружению атак и реагированию на них позволяет минимизировать частоту инцидентов и ущерб. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена угроза, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.

Расследование инцидентов: Research Graph ускоряет расследование инцидентов, позволяя визуально изучать хранящиеся в Threat Lookup данные и обнаружения; дает графическое представление связей между веб-адресами, доменами, IP-адресами, файлами и другими данными для иллюстрации полного масштаба инцидента и выявления его основной причины.

Мастер-поиск: поиск информации с использованием всех активных сервисов анализа угроз и внешних источников (включая индикаторы компрометации из открытых источников, а также поиск в теневом и поверхностном интернете) в едином и мощном интерфейсе.

Простота использования через веб-интерфейс или REST API: сервисом можно пользоваться в ручном режиме через веб-интерфейс (в браузере) или через REST API.

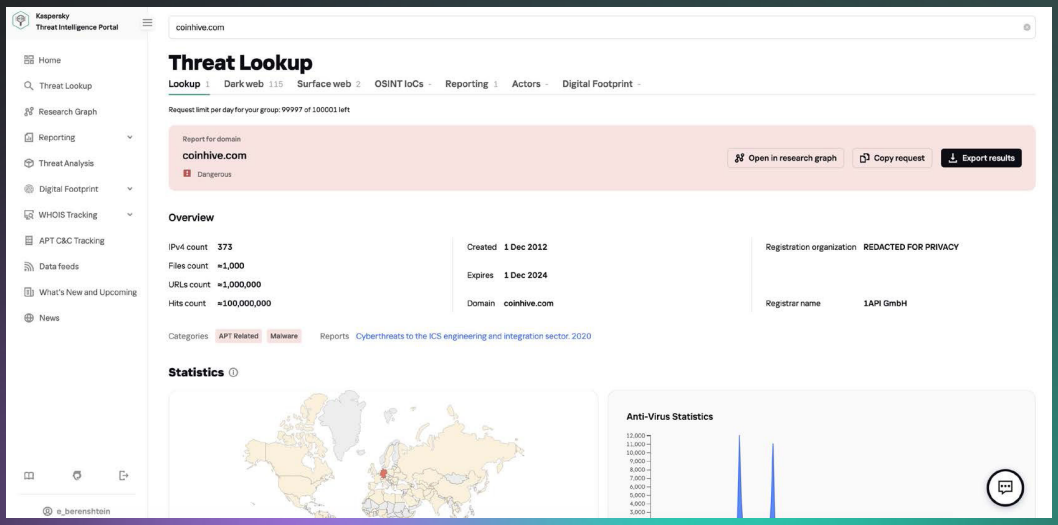
Разнообразие форматов экспорта: поддерживается экспорт индикаторов компрометации и контекстных данных в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, YARA, Snort и CSV. Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти сведения в системы управления безопасностью, такие как SIEM.

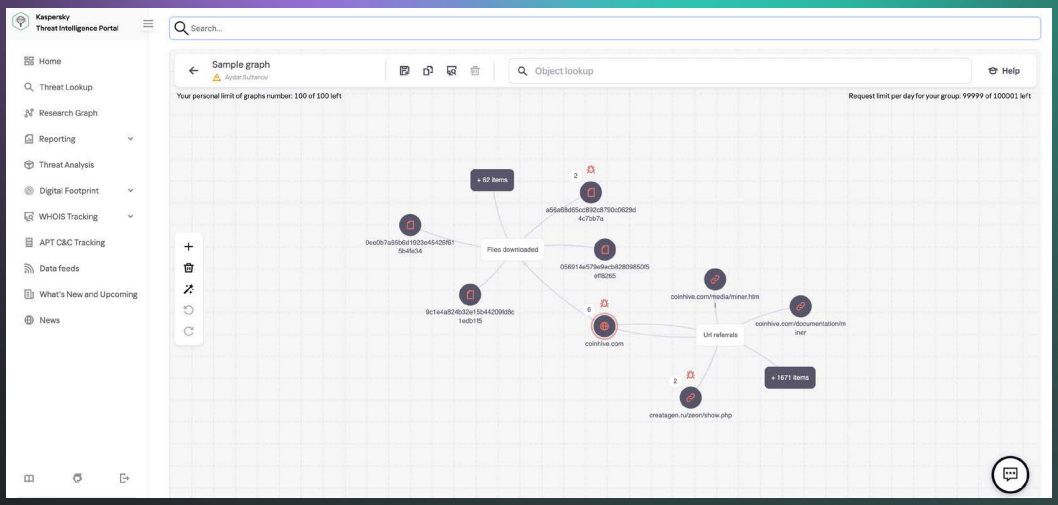
Ценность

Глубокий анализ индикаторов угроз с помощью проверенной контекстной информации позволяет приоритизировать атаки и сосредоточиться на устранении угроз, представляющих наибольший риск для бизнеса.

Эффективная и результативная диагностика и анализ инцидентов безопасности на узлах и в сети. Приоритизация сигналов о неизвестных угрозах от внутренних систем.

Улучшение процесса реагирования на инциденты и расширение возможностей поиска угроз, позволяющее прервать цепочку развития угрозы до момента компрометации критически важных систем и данных.





Платформа поможет:

Найти информацию об индикаторах угроз с помощью веб-интерфейса или REST API.

Выяснить, является ли обнаруженный объект распространенным или уникальным.

Понять, почему объект считается вредоносным.

Получить подробные сведения об объекте, включая сертификаты, распространенные названия, пути файлов и веб-адреса, для выявления новых подозрительных объектов.

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru